

CLAIMS

What is claimed is:

- 1 1. A method for prioritized network security, comprising:
  - 2 (a) identifying a set of policies, each policy having a condition associated therewith;
  - 3 (b) determining whether the conditions are met; and
  - 4 (c) activating the policies whose associated conditions are determined to be met;
  - 5 (d) wherein the conditions represent a priority of the policy.
- 1 2. The method as recited in claim 1, and further comprising determining whether a  
2 user confirms the activation of the policies.
- 1 3. The method as recited in claim 2, and further comprising activating the policies  
2 if the user confirms.
- 1 4. The method as recited in claim 1, and further comprising updating the set of  
2 policies.
- 1 5. The method as recited in claim 4, wherein the updating includes receiving  
2 another inactive policy, determining whether the user accepts the inactive policy,  
3 and adding the inactive policy to the set if the user accepts the inactive policy.
- 1 6. The method as recited in claim 1, wherein the activation of the policies includes  
2 adding the policies to a set of a plurality of active policies, and executing  
3 security actions associated with the active policies if associated limits are met.

1 7. The method as recited in claim 6, and further comprising determining whether  
2 the conditions associated with the active policies are still met, and de-activating  
3 the active policies if the associated conditions are not met.

1 8. The method as recited in claim 6, and further comprising identifying currently  
2 executed security actions, determining whether a conflict exists between the  
3 currently executed security actions, and resolving any conflicts between the  
4 currently executed security actions.

1 9. The method as recited in claim 1, wherein the conditions include a time factor.

1 10. The method as recited in claim 1, wherein the conditions include a source of the  
2 policies.

1 11. The method as recited in claim 1, wherein the conditions include a severity of  
2 security actions associated with the policies.

1 12. A computer program product for prioritized network security, comprising:  
2 (a) computer code for identifying a set of policies, each policy having a condition  
3 associated therewith;  
4 (b) computer code for determining whether the conditions are met; and  
5 (c) computer code for activating the policies whose associated conditions are  
6 determined to be met;  
7 (d) wherein the conditions represent a priority of the policy.

1 13. The computer program product as recited in claim 12, and further comprising  
2 computer code for determining whether a user confirms the activation of the  
3 policies.

1 14. The computer program product as recited in claim 13, and further comprising  
2 computer code for activating the policies if the user confirms.

1 15. The computer program product as recited in claim 12, and further comprising  
2 computer code for updating the set of policies.

1 16. The computer program product as recited in claim 15, wherein the updating  
2 includes receiving another inactive policy, determining whether the user accepts  
3 the inactive policy, and adding the inactive policy to the set if the user accepts  
4 the inactive policy.

1 17. The computer program product as recited in claim 12, wherein the activation of  
2 the policies includes adding the policies to a set of a plurality of active policies,  
3 and executing security actions associated with the active policies if associated  
4 limits are met.

1 18. The computer program product as recited in claim 17, and further comprising  
2 computer code for determining whether the conditions associated with the active  
3 policies are still met, and de-activating the active policies if the associated  
4 conditions are not met.

1 19. The computer program product as recited in claim 17, and further comprising  
2 computer code for identifying currently executed security actions, determining  
3 whether a conflict exists between the currently executed security actions, and  
4 resolving any conflicts between the currently executed security actions.

1 20. The computer program product as recited in claim 12, wherein the conditions  
2 include a time factor.

1 21. The computer program product as recited in claim 12, wherein the conditions  
2 include a source of the policies.

1 22. The computer program product as recited in claim 12, wherein the conditions  
2 include a severity of security actions associated with the policies.

1 23. A system for prioritized network security, comprising:  
2 (a) logic for identifying a set of policies, each policy having a condition associated  
3 therewith;  
4 (b) logic for determining whether the conditions are met; and  
5 (c) logic for activating the policies whose associated conditions are determined to be  
6 met;  
7 (d) wherein the conditions represent a priority of the policy.

1 24. A method for prioritized network security, comprising:  
2 (a) identifying a set of policies each having an associated security action and a limit  
3 for triggering the security action;  
4 (b) determining whether the limits are met;  
5 (c) executing the security actions of the policies whose associated limits are  
6 determined to be met;  
7 (d) identifying currently executed security actions;  
8 (e) determining whether a conflict exists between the currently executed security  
9 actions; and  
10 (f) resolving any conflicts between the currently executed security actions.

1 25. The method as recited in claim 24, wherein each policy has an associated  
2 priority, and the conflicts are resolved based on the priority.

- 1 26. A method for prioritized network security, comprising:
- 2 (a) identifying a set of security actions, each security action having a limit and a
- 3 priority associated therewith;
- 4 (b) determining whether the limits are met; and
- 5 (c) executing the security actions whose associated limits are determined to be met;
- 6 (d) wherein the security actions are executed based on the priority.

- 1 27. A method for prioritized network security, comprising:
- 2 (a) identifying a set of policies, each policy having a condition and a priority
- 3 associated therewith;
- 4 (b) determining whether the conditions are met; and
- 5 (c) activating the policies whose associated conditions are determined to be met;
- 6 (d) wherein the policies are activated based on the priority.

- 1 28. A method for prioritized network security, comprising:
- 2 (a) identifying a set of policies, each policy having a condition associated therewith;
- 3 (b) determining whether the conditions are met; and
- 4 (c) activating the policies whose associated conditions are determined to be met;
- 5 (d) wherein the conditions represent an urgency associated with an issue causing the
- 6 policy to be activated.

- 1 29. A method for providing network security, comprising:
- 2 (a) identifying a set of a plurality of inactive policies each including a security
- 3 action, a condition for activating the policy, and a limit for triggering the security
- 4 action if the policy is active;
- 5 (b) updating the set of inactive policies including:
- 6 (i) receiving another inactive policy,
- 7 (ii) determining whether the user accepts the inactive policy, and

- 8 (iii) adding the inactive policy to the set if the user accepts the inactive
- 9 policy;
- 10 (c) determining whether the conditions are met for the inactive policies;
- 11 (d) determining whether a user confirms the activation of the inactive policies if the
- 12 associated conditions are met; and
- 13 (e) activating the inactive policies if the user confirms, the activation including:
- 14 (i) adding the inactive policies to a set of a plurality of active policies,
- 15 (ii) determining whether the conditions associated with the active policies
- 16 are still met,
- 17 (iii) de-activating the active policies if the associated conditions are not met,
- 18 and
- 19 (iv) executing the security actions associated with the active policies if the
- 20 associated conditions are met and the limits are met, the execution of the
- 21 security actions including:
- 22 (1) identifying currently executed security actions,
- 23 (2) determining whether a conflict exists between the currently
- 24 executed security actions, and
- 25 (3) resolving any conflicts between the currently executed security
- 26 actions.
- 27